AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method to facilitate locking an adversary out of a network application, comprising:

receiving at a server a request, including an authentication credential, to access the network application, wherein the authentication credential includes a user identifier ~~associated with a user~~ and a specific network address of a user device;

~~examining an audit log to determine if the user identifier has been locked out from the specific network address; and~~

if the user identifier has been locked out from the specific network address,

denying access to the network application; and

~~otherwise, checking the authentication credential for validity, and~~

if the authentication credential is valid,

allowing access to the network application,

otherwise,

logging a failed attempt in the audit log,

imposing a lockout for the user identifier from only the specific network address after a threshold number of failed attempts from the specific network address, if a threshold number of specific network addresses are locked out for the user identifier, imposing a global lockout for the user identifier, and

denying access to the network application~~;~~

~~whereby the adversary is prevented from accomplishing an attack by masquerading as the user~~.

2 (Canceled).

3. (Previously presented) The method of claim 1, further comprising: removing a lockout after a predetermined period of time.

4. (Previously presented) The method of claim 1, further comprising: manually removing a lockout by an administrator of the server.

5. (Original) The method of claim 1, wherein the authentication credential includes a user name and a password.

6. (Original) The method of claim 5, wherein checking the authentication credential for validity involves:

verifying that an administrator has authorized access to the network application for a combination of the user name and the password; and

determining if the request violates an access rule in a rule table.

7. (Original) The method of claim 6, wherein the access rule can specify:

an allowed time-of-day;

an allowed number of access attempts;

an allowed network address; and

an allowed network domain.

8. (Original) The method of claim 1, wherein the network address includes an Internet Protocol address.

9. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method to facilitate locking an adversary out of a network application, the method comprising:

receiving at a server a request, including an authentication credential, to access the network application, wherein the authentication credential includes a user identifier ~~associated with a user~~ and a specific network address of a user device;

~~examining an audit log to determine if the user identifier has been locked out from the specific network address; and~~

if the user identifier has been locked out from the specific network address,

denying access to the network application; and

~~otherwise, checking the authentication credential for validity, and~~

if the authentication credential is valid,

allowing access to the network application,

otherwise,

logging a failed attempt in the audit log,

imposing a lockout for the user identifier from only the specific network address after a threshold number of failed attempts from the specific network address, if a threshold number of network addresses are locked out for the user identifier, imposing a global lockout for the user identifier, and

denying access to the network application~~;~~

~~whereby the adversary is prevented from accomplishing an attack by masquerading as the user~~.

10 (Canceled).

11. (Previously presented) The computer-readable storage medium of claim 9, the method further comprising: removing a lockout after a predetermined period of time.

12. (Previously presented) The computer-readable storage medium of claim 9, the method further comprising: manually removing a lockout by an administrator of the server.

13. (Original) The computer-readable storage medium of claim 9, wherein the authentication credential includes a user name and a password.

14. (Original) The computer-readable storage medium of claim 13, wherein checking the authentication credential for validity involves:

verifying that an administrator has authorized access to the network application for a combination of the user name and the password; and

determining if the request violates an access rule in a rule table.

15. (Original) The computer-readable storage medium of claim 14, wherein the access rule can specify:

an allowed time-of-day;

an allowed number of access attempts;

an allowed network address; and

an allowed network domain.

16. (Original) The computer-readable storage medium of claim 9, wherein the network address includes an Internet Protocol address.

17-24 (Canceled).